Crisis management in extreme situation: the model of resilience in situation (MRS) as a support to observe the organization with simulation

Cecilia DE LA GARZA, Quentin Baudard, Pierre Le Bot

Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Crisis management in extreme situation: The Model of Resilience in Situation (MRS) as a support to observe the organization with simulation

Q. Baudard, P. Le Bot & C. De la Garza
EDF Research and Development, Human and Organizational Factors Group

ABSTRACT: The traditional approach to safety engineering for a nuclear reactor is mainly focused on its technical dimension, while the Human Factors approach focuses on how to optimize the value added by human to the reliability of the system. Safety management seeks to organize the work as well as possible, train employees, develop their safety culture, and so on. This juxtaposition of approaches to reliability illustrates the recurring dilemma faced by at-risk organizations in choosing between the technical anticipation of pre-defined situations and the optimization of the management of the situations by people who, in real time, through their skills and understanding of the situation going on, will adapt their strategy and actions according to that particular situation. These last three years, we have performed a series of Extreme Situation Simulations on Full Scale Simulators in order to test the resilience of the Crisis Organization of EDF during accidents with characteristics similar to the accident of Fukushima. The realization of these tests was an organizational challenge which required up to 80 people for the simulation, and about 5 months for both the preparation and the analysis of the tests.

1 OBJECTIVE OF THE STUDY

Following the Fukushima accident, EDF implemented additional crisis management measures (organizational, material, etc.) to respond to an accident in an Extreme Situation (ES). An Extreme Situation is a situation in which a nuclear site is isolated and inaccessible as consequences of a large-scale external event which has an impact on all the reactors of the site, and during which the operating teams have limited means of communication. The objective of our works was to study the design of the operating teams in Extreme Situations and the National Crisis Management Organization of EDF, in order to identify the strengths and the areas of improvement for crisis management.

To do this, we observed simulations involving the entire crisis management organization of EDF, which would operate in an ES, from the operating teams on-site, to the experts from the National Technical Support Team, along with members of the National Direction Command Post. External stakeholders (Public Powers, Regulatory Authority…) have not been taken into account in the simulation.

We applied a multidisciplinary approach to these simulations, cross-referencing the analyses of experts in Cognitive Ergonomics, Human Reliability and Nuclear Safety. Our method of analysis of these simulations is based on the Model of Resilience in Situation (Le Bot & Pesme, 2010), which explains how a socio-technical system such as the one we have observed can continue to operate safely using a process of anticipation and a process of adaptation. Therefore, beyond the operational objective of studying the organizational system anticipated in an ES, we examined more closely the link between resilience and crisis management.

The purpose of this communication is to present the method we have developed for the implementation of the Extreme Situation Tests and the one used for their analysis. We will first see how the specific context of an ES is complex to simulate, and how we managed to achieve it. We will then detail the method of observation of the tests and analysis, focusing on the functional analysis of the resilience in accordance with the Model of Resilience in Situation. Finally, we will present some of the conclusions we have drawn from the analyses and the first lessons for the implementation of simulations.

2 TESTS IN EXTREME SITUATIONS

2.1 *What is an extreme situation?*

The concept of Extreme Situations emerged following the accident at Fukushima in 2011. The situation we considered as representative for the study of the crisis organization is a situation with characteristics similar to this one.

We suppose that a nuclear site is hit by a major earthquake leading to the loss of internal and external power supplies on at least two reactors, with the isolation of the site preventing the immediate arrival of the local on-call emergency response teams and the Safety Engineer.

Furthermore, nearly all internal and external communication systems of the site have been rendered unavailable by the event: in the first tests, the control room could not communicate remotely with the field operators when they are working on field manoeuvers. In later tests, an autonomous communication system was available for the teams to communicate with the field operators. In the short-term, the team in the control room can only receive support from the National Emergency Response Team by communicating with the "National Direction Command Post" via an emergency satellite telephone.

2.2 *How to simulate an extreme situation?*

During our study, we observed two series of three tests, each involving complete operating teams on full scale simulators. Four tests were carried out on two simulators in parallel, representing a beyond-design-basis "multi-unit" site accident, simultaneously affecting two reactors on one site. During one of these exercises, the two simulated units were of different technologies. The two remaining tests were focused on thermohydraulic design basis accidents in situations combined with another event (fire or flooding), in order to study the design of the team in a non-isolated site situation.

A multi-disciplinary work group, consisting of representatives of the site operations departments, training instructors on simulators and experts on ergonomics, human reliability and safety, prepared the tests. This group produced the test protocol and defined a scenario able to provide sufficient data to understand crisis organization in a beyond-design-basis extreme situation. The accident scenarios were tested and validated in technical and documentary terms, and lastly, for each test, a prior "dummy" test was used to check the entire simulation system with site operating teams.

This study meant that for the first time within the company, tests could be performed on two full scale simulators in parallel built in the training centre of the sites, a "hardware" one reproducing the control room exactly, and another "digital" one with touch screens representing the devices of the control room. During one of the tests, a third unit was simulated on paper: it was a world's first. The simulation of several units raises numerous problems, for example, certain units are paired and share common equipment. This is not the case for the full scale simulators, they are technically independent. Thus, during tests simulating two paired reactors sharing common systems, the unavailability of shared equipment needed to be simulated for one simulated reactor if the other simulated reactor used it.

Furthermore, following the Fukushima accident, it was decided to equip each reactor with complementary equipment for facing extreme situations, such as emergency unit cooldown diesel generator sets: these were not yet taken into account in the simulators, or in the training of the operating teams at the time of the tests. Since the objective of the simulations is to study the operation of the crisis organization as it would be with this equipment deployed, these devices were provisionally simulated for the tests and the operating teams participating in the tests were specially prepared in their use. The validation of the new procedures was not an objective of the tests.

Lastly, it emerged from our preliminary analyses of the Fukushima accident (Baudard, 2017) that the field actions had played a very important role in the crisis management. We therefore involved the field operators of each operating team in the simulation by asking them to simulate the completion of the actions requested by the control room in a degraded environment (poor lighting, access path blocked, etc.). This participation by the field operators helped to ensure a more realistic simulation, even though they have not simulated their actions directly in the field.

2.3 *The observation system*

To limit as far as possible any technical contingencies in the progress of the test, each scenario was played out twice with different teams before being observed during the final test. The aim of these precautions was to seek possible faults in the procedures

Table 1. Data collection methods.

In-situ observation	Ergonomics	Human reliability
Note taking	Chronologies, actions performed, decision making, communication, difficulties observed.	
Video & audio recording	Detailed subsequent analysis of sequences chosen	Used only in case of doubt
Types of instrumented collection		Process evolution Logbooks
Post-simulation debriefings	Debriefing focused on the Notable Events in the organization, noted during the observation and discussed between observers during the preparation of the debriefing	

which were being designed, but also to allow the trainers to adapt to this unusual scenario.

The tests involved up to 80 people, from its preparation through to the implementation:

- two complete operating teams and one observer per team member
- field operators for each team and one observer per group
- the experts of the national Technical Support Team and two dedicated observers
- members of the National Direction Command Post and two dedicated observers
- Scenario creators and trainers
- In-house specialists and others from outside of the company coming to observe the method of data collection
- etc.

The system observed is adapted to the crisis organization which would take place in an ES in order to represent it as accurately as possible. However, entities from outside of the company (prefecture, regulatory agency, media, etc.) were not simulated. The system is characterized by the six observation posts (two simulators, two teams of field operators, the National Technical Support Team (NTST) and National Direction Command Post) across which the ergonomics, human reliability and safety observers were spread. The simulation takes place over a period of five hours, followed by an on-the-spot debriefing and post-analysis of the simulator logbook. The data collection methods are detailed in the following table:

Five work themes guided the organization, the observation and the analysis of the Extreme Situation Simulations:

- The design of the operating team
- Field actions management
- Information Exchange with the National Crisis Organisation
- The use of the tools and resources available in an ES
- The resilience of the organisation, which we will look at in more detail later.

3 DATA ANALYSIS

3.1 *Analysis method*

The main stages in the analysis method are summarized in Table 2 below:

Following the observation of a test, the multidisciplinary analysis group identifies the favorable and unfavorable factors for the organizational resilience of the socio-technical system in Extreme Situations. The common document base for analysts is as follows:

- The exhaustive chronologies by group (operating team, Technical Support Team, etc.) is reproduced based on the notes taken by each observer, distinguishing the actions carried out by the group (application of procedures, launching field actions, etc.) and events independent of the group (equipment failure, action carried out by an independent group, etc.)
- Identification of "Notable Events" (NE). A Notable Event is an event or the repetition of an event which reveals an action, the absence of an action, a decision made, a collective or individual initiative, a fact that can strengthen the reliability of the organisation of the operating team, and/or the emergency response team, operations, its robustness, facilitating sensemaking, or on the contrary which may make the socio-technical system less reliable and make safety barriers more fragile, damaging sensemaking. The NE are observed during the in situ observation, subsequently during the group debriefing, or during the reconstruction of the overall chronology. NE are the central elements in the analysis of the resilience of the socio-technical system.

The NE are then categorized according to the groups they refer to (control room 1 or 2, emergency response team, management control unit, field operators), and a first level of analysis is used to identify:

- the Technical NE, resulting from operations on the process

Table 2. Contribution of the different disciplines to the analysis of the situations.

					Ergonomics		
Observers	Human reliability + ergonomics		Human reliability		Cognitive analyses and analyses of group operations		
Chronology by observer, then by Group, then overall chronology	Raw analysis from observations and debrefings Notable Events	Technical points Summary of notable events by group and overall	Monacos chronologies progress of operations	Functional analysis of resilience	Timing charts of control room activity and Site/ National interactions	Themed analyses of debriefings	Analysis by hypothesis

- the Expertise NE on the assistance that the experts provide for the operations
- the Organizational NE on the operation of the group as a whole.

Lastly, the Human Reliability analysts link together the Notable Events, the characteristics of the system observed, and the resilience functions defined in the MRS.

3.2 *Model of resilience in situation*

The Model of Resilience in Situation (Le Bot & Pesme, 2010) is an empirical model which was build out of analyses of real or simulated accidents, based on the theoretical framework of Social Regulation (Reynaud, 1997). The model serves to reconcile two seemingly opposite rationales: the anticipation of potential situations on the one hand and adaptation to the situation on the other. It is used to dynamically describe the operational management of a crisis situation, alternating between periods of constructing ad'hoc operating rules and periods of application of these rules. Should the rules being applied become obsolete, the process will repeat.

The MRS applies to crisis organization as a whole, as a dynamic network of work groups (operating team, experts, etc.) that interact, cooperate, collaborate and coordinate themselves. Each of these groups, taken within its own environment (procedures, HMI, etc.), is considered a distributed cognitive interactive system. The overall resilience of the organization therefore results from interactions within the groups and interactions between groups.

The model links together two processes: the execution process, and the adaptation process based on Figure 1:

In stable operating conditions, the system executes the operation rules (EXECUTION). The functions to be performed continuously are:

– INFORMATION: selection and sharing of information based on the surveillance criteria
– ACTION: act based on the objectives and their priorities with the corresponding resources
– CONTROL: ensure that the action complies with the operating rules

If the continuous VERIFICATION detects that the rules are not appropriate or are obsolete (objective achieved), the system initiates a Rupture phase after a RECONFIGURATION: interruption of the rules which are not relevant, mobilization of resources, then ADAPTATION in order to readjust the operating rules by carrying out DIAGNOSIS, PROGNOSIS, SELECTION of relevant procedures and parameters, PRIORITISATION of objectives, COLLABORATION to negotiate and define the operating rules, COOPERATION to distribute the tasks and the resources.

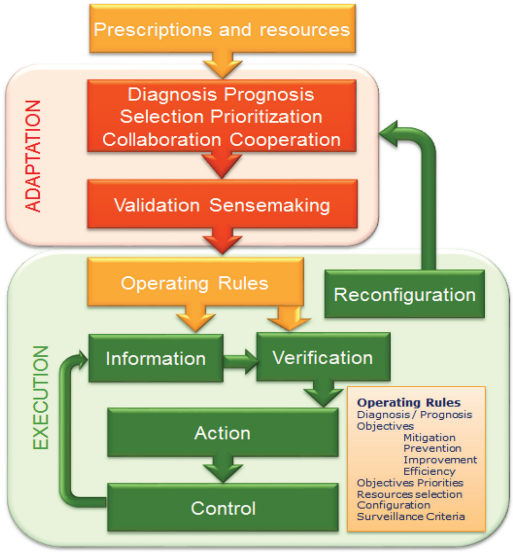

Figure 1. The model of resilience in situation.

The operating rules are validated (VALIDATION) and shared to make the situation relevant, implementing them and linking the past experience, present actions and future projections of the parties involved.

3.2.1 *Definitions of the MRS functions*

Adaptation process:
The adaptation process involves redefining operation: objectives, strategy and resources to achieve the objectives. This means:

– Anticipating the behaviour of the installation and the actions to be carried out (diagnosis and prognosis functions)
– Selecting the relevant information, procedures, instructions and means/resources (selection function)
– Collaborating to adapt them autonomously if necessary, to define the new strategy with the operational objectives and resources (collaboration and prioritisation functions)
– Validating the implementation of the rule by the authorised party (validation function).

Execution process:
The execution process involves robustly implementing the agreed strategy:

– The robustness is obtained by the execution (action function) and the control of the ongoing actions (control function).

– The group constantly checks that this strategy remains appropriate in regard of the situation (verification function)
– These functions are carried out by the acquisition and the sharing of information (information function), and guided by sensemaking (sensemaking function)

3.3 *Functional analysis of resilience*

During our analyses of the tests, we seek to relate Notable Events with these resilience functions and estimate whether they are favorable or unfavorable. For example, the contribution of a member from outside of the operating team to the production of the rules to be followed is a favorable factor for COLLABORATION between groups. On the contrary, the workload of parties involved in Extreme Situations slowed down the management of field actions, which was an unfavorable factor for the ACTION and CONTROL functions to be carried out, as well as for the PRIORITISATION of actions.

Our analysis can be summarized by the diagram on Figure 2. Taking the example of the use of a new field actions management tool, the Field Actions Monitoring Device, we would have the analysis on Figure 3.

This tool was introduced in the second series of tests, trying to resolve the difficulties observed. More specifically, its use in extreme situations allowed us to observe that the tool ensured that the field actions to be carried out were managed correctly. With minimal preparation in this new tool, the team was able to implement organization ensuring effective management of field actions, particularly important in an ES. Furthermore, this tool facilitates the prioritization of field actions and the monitoring of field operators and their optimization in a situation requiring many field actions. Therefore, the Field Actions Monitoring Device was a favorable factor in controlling the state of the reactor in a degraded situation.

4 GENERAL DISCUSSION

The results of our analyses show that the design basis of the crisis management organization in Extreme Situation was not called into question. It also appears that some observed difficulties require more consideration in the preparation of the operating teams in order to strengthen resilience.

4.1 *Management of field actions*

The main observation relates to the management of field actions and of the "field operator" resources. In a design basis accident, if electrical power sources are lost, the necessary number of safety-related equipment items for the facility are backed up by Emergency Diesel Generators and can still be controlled remotely in the control room. Field actions then involve trying to return the systems to service or checking the shutdown of the stopped systems, and therefore these actions are not generally essential for the operation of the reactor. In an Extreme Situation with a beyond-design-basis

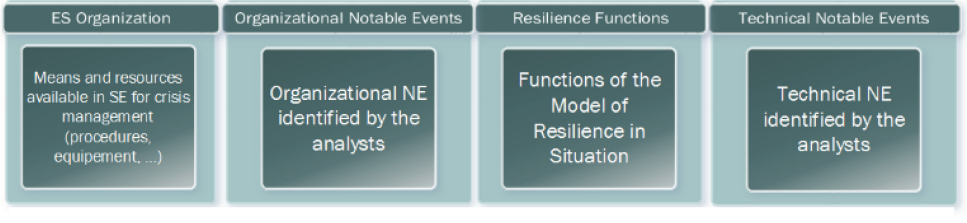

Figure 2. Functional analysis of resilience method.

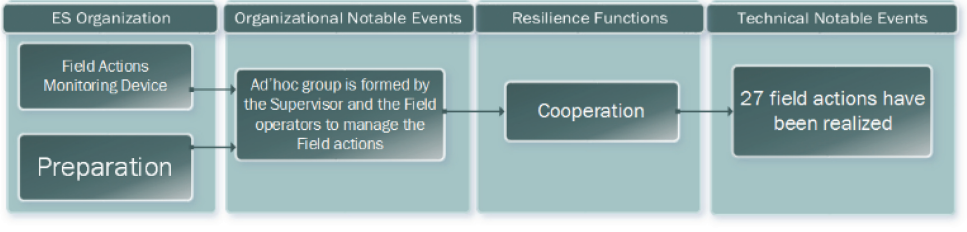

Figure 3. Example of functional analysis of resilience method: Field actions monitoring device.

loss of electrical power sources, these backups may be lost and the operation of the installation may require direct field action to control certain equipment, try to return it to service or take information. The field operators are in fact in high demand. They are sent in the field on a case-by-case basis depending on each action demanded by the team in the control room, with one or more field action sheets, and their actions are not carried out instantly since they need to travel to the premises before executing their sheet, and the action itself must often be executed manually. Each sheet therefore requires human resources, one or more field operators will need time to perform the action demanded.

Prioritizing and re-prioritizing the field action sheets becomes a condition for the success of the crisis management in the control room. This activity has considerable cognitive requirements for the person responsible of it, and an impact on the collective operation of the team. During our tests, this activity takes up a lot of the supervisor's time, therefore leaving them less available for the team and for their own supervision tasks.

To help to manage the field actions and the field operators, a prototype of a Field Actions Monitoring Device has been designed as part of an agile process (De la Garza et al., 2016). This is a triptych panel providing an overview of the actions pending, allowing them to be prioritized and then to see those which are in progress and who is carrying them out, and finally the successes and failures. This system is a support for ES operation, making it easier to monitor and ensure the safety of the field operators who leave to carry out actions. It also allows information to be shared within the operating team and becomes an area for exchanges, or even collective problem-solving.

4.2 *Reflections on the ES simulation system*

The organization and analysis of an Extreme Situation test is costly in terms of time and resources: 60 to 80 people from different entities (operators, engineering, trainers, R&D, etc.) working on the organization and progress of the tests requiring 4 to 6 months of preparation, then 4 to 6 months of analysis… We have adopted a procedure of continuous improvement in the organization of the tests, progress of which has been spread over more than three years, getting the various stakeholders in the preparation involved earlier in the process, and optimizing the analysis method.

However, we can see that there remain questions pending and areas for improvement to be followed in the organization of simulations on such a large scale, and in particular based around four points discussed above relating to the preparation, creation of scenarios and control of certain variables.

4.2.1 *Unpredictability of the scenario*

The scenario we designed for the tests was a succession of equipment failures (loss of off Site Power, Loss of on-site Power…) similar to the damages that the Fukushima Daiichi NPP faced during the crisis. In order to successfully manage the accident, the operating teams have to apply rarely used procedures.

Before the final test, we had to validate the technical aspects of de simulation, like the behavior of the Full Scale Simulator in this situation where it had to cope with a lot of equipment failures, or how well the procedures matched with the situation.

The problem is that, because of the autonomy we gave to the operating teams during the simulations, if we want to validate the adequacy of the procedures, we have to make sure that they are correctly applied by the operating team: operators might choose another procedure to apply, if they consider it more appropriate. Instructors however are trained to strictly apply the procedures, so we preferred having them for the technical validation of the scenarios.

Even though the technical validation is necessary, it does not protect from problems during the test. But since their objective was to study the resilience of the teams, we left them a lot of autonomy in the operations, and we would not have stopped the simulation should they have applied a procedure we had not expected.

4.2.2 *Simulating equipment which is scheduled but not yet installed*

How can the players be prepared to manage a simulation which will require equipment and an organization which are not yet scheduled as part of their training, and at the same time make the situation as close as possible to the target? Here we have a modification of an existing situation.

To train the teams, we offered them preparatory information meetings, during which the objective of the tests, the scheduled progress for the day and the new systems scheduled for crisis management were presented, without giving them any indication of the scenario which would be played out.

Research is in progress at EDF on rapid means of prototyping control room interfaces, which can be combined with the simulator design codes. The equipment scheduled as part of the post-Fukushima project could therefore be integrated into the simulators during extreme situation tests.

4.2.3 *Getting the players involved*

How can the players get involved in the simulation of a faulted condition, in a highly-degraded environment?

It is of course impossible to recreate in the control room or in the field the degraded condi-

tions encountered by the operators during the Fukushima accident. However, using field operators, we regularly provided the control room with information on the degraded state of the facilities. For example, on returning from a simulated field inspection, the field operator drew up for the supervisor the list of inaccessible premises, damaged equipment, etc.

We have seen tests in which the teams attached great importance to the safety of the participants in the field, avoiding sending them for field actions which are irrelevant given the situation, or sending them in pairs. These observations were interpreted as a good understanding of the situation in hand.

It has however not always been clear in the mind of the teams that the site was isolated, to the extent that some were waiting for the arrival of the on call teams in order to launch important actions. The question arises of how to simulate the consequences of the external hazard on the environment of the plant which have a major impact for the operators and their actions.

4.2.4 *Importance of multi-reactor accident simulations*

Our studies into the Fukushima accident highlighted the interactions which took place between the different damaged units on the site (Baudard, 2017): immobilization of resources, focus on one reactor at the expense of the others, transfer of experience, etc.

Thanks to the autonomy we left to the teams, they were able to perform out of the procedures actions, and we identified transfer of experience mechanisms during the simulations. For example, one operating team benefited from the experience of the team from the neighboring plant unit in restoring the power supply using the backup means scheduled in the post-Fukushima provisions.

Our work on the ES tests highlighted favorable factors allowing these beyond-design-basis crisis situations to be managed, but there are also factors which will require progress. Since these simulation of multi-units accidents are relatively recent, we think that it would be helpful, for understanding and improving resilience, to develop these simulation situations, but also simplifying them.

4.3 *Our proposition for future preparations*

Indeed, even though the organization, observation and analysis of the tests have been highly beneficial for the development of knowledge on Extreme Situations management by the parties involved within the company, these tests are too costly and too time consuming.

We have already started investigating lighter simulation methods for the teams involved in crisis management (through Serious Games or Storytelling for example), focusing on one specific group rather than the whole organization, and simulating its environment. A prototype has been tested with the National Technical Support Team (Alengry et al, 2018).

REFERENCES

Alengry, J. et al 2018. What is "training to cope with crisis management situation"? A proposal of a reflexive training device for the National Technical Support Team. *International Ergonomics Association*.

Baudard, Q. & Le Bot, P. 2017. Modelling Human Operations during a nuclear accident: The Fukushima Daiichi accident in light of the MONACOS Method. In Marko Cepin, Radim Bris (ed), *Safety and Reliability Theory and Application, ESREL Proceedings 17–21 June 2017*. CRC Press, Balkema.

De La Garza et al, 2016. D'un « document » à un « dispositif » de suivi des actions en local dans le nucléaire. *Ergo'IA 2016*.

Le Bot, P. & Pesme, H. 2010. The Model of Resilience in Situation (MRS) as an Idealistic Organization of Atrisks Systems to be Ultrasafe. *PSAM10–10th International Conference on Probabilistic Safety Assessment & Management*.

Reynaud, J.D., 1997. Les Règles du jeu: L'action collective et la régulation sociale, *Armand Colin, Paris, 1997.*